REMARKS

In the Office Action the Examiner objected to the title for not being descriptive, objected to the abstract as having an informality, objected to claims 1-7, 14-18 as having informalities, rejected claims 15-17 under 35 U.S.C. 112, second paragraph as being indefinite, and rejected claims 1-18 under 35 U.S.C. 103 as being obvious. Claims 1-18 remain in the application.

The Examiner's objection to the title has been addressed by an amendment thereto.

The Examiner's objection to the abstract was for having the title of the application above the heading. Applicants have no objection to removing the title but point out that requiring such removal is contrary to current USPTO practice. Countless patents have been filed with the title above the heading on the abstract page without objection.

The Examiner's objection to claims 1-7 and 14-18 is based on the preamble of these claims containing the phrase "message digest hardware accelerator." The Examiner suggested using "apparatus" instead, which has been adopted.

The Examiner's rejection of claims 15-17 has been obviated by amending these claims. The amendment to claim 15 prompted the amendment to claim 16. Claim 17 was amended by making it depend on claim 15 and by another small change.

The Examiner's rejection for obviousness used Child as the primary reference. Child discloses a circuit that performs a single type of hash function (SHA) serially instead of applicants' parallel approach that can also selectively perform more than one type of hash function. Applicants' approach is both faster and requires less space on the integrated circuit.

With regard to claim 1, the Examiner used Childs and four additional references, Ober, Schneier, Turner, and Batcher, to come to conclusion that claim 1 was obvious to one or ordinary skill in the art. The claimed first multiplexer is useful in allowing for the use of the register file for both hash modes. The Examiner states that this claimed first multiplexer is obvious because multiplexers are known to switch between a signal and a reference and that this claimed location in the circuit is obvious because there is an incentive to minimize the number of elements. In effect the Examiner is saying two things: (1) one of ordinary skill in the art would recognize the benefit of applicants' invention and (2) anytime known elements are used to achieve a benefit that is recognizable to one of ordinary skill in the art, it is obvious for one of ordinary skill in the art to have done so. Applicants agree with the first but not the second. The Examiner's application of the legal requirement for an incentive to combine implies that anytime

a circuit that uses transistors of the type known in the art for switching or amplification and such circuit provides a known desired benefit such as reducing circuit elements or improving speed, such circuit is obvious and unpatentable. In this case there is no suggestion in the prior art that the elements that are combined by Applicants can be combined in the manner claimed by Applicants. Ober teaches that both hash functions can exist on the same integrated circuit, but applicants have not been able to find any reference that there is any suggestion that these two functions can share the same circuitry much less teach which elements can be shared. The Examiner is applying hindsight using Applicants' teaching to construct from the prior art the resulting claimed circuits. Accordingly, applicants submit that claim 1 patentably distinguishes over the five reference combination applied by the Examiner.

With regard to claims 2-7, the Examiner continued to apply the same approach that because Applicants used known circuit elements in achieving the result and the result was beneficial, the result was obvious. Applicants disagree as stated above.

Independent claim 8, as amended, claims an adder with a first, second, third, fourth, and fifth input. Childs discloses a two input adder 522. Notice that applicants' circuit does not require multiplexer 501 and flip-flops 502-506. Childs needs these flip-flops as temporary storage for chaining variables. This makes the operation significantly slower. Further, these flip-flops require more space than the additional space required over a two input adder. Also multiplexer 520 is not required and accumulator 523 is not used. There are multiplexers used to control the inputs to the five input adder, but these are for the different modes, SHA-1 and MD5. Once the mode is selected these multiplexers simply feedthrough the input for that mode. There is no switching between inputs to the adder during the determination of the hash output. In Childs, multiplexers 521 and 520 are switching inputs (serial approach) to adder 522 during the determination of the hash output, thus being significantly slower in determining the hash output than applicants' five input adder (parallel approach) manner of performing the hash function. Accordingly, applicants submit that claim 8 is patentably distinct from the art cited by the Examiner.

With regard to claims 9-13, the Examiner continued to apply the same approach used against claim 1 that because Applicants used known circuit elements in achieving the result and the result was beneficial, the result was obvious. Applicants disagree as stated above.

With regard to independent claim 14 and dependent claims 15-18, the Examiner used the same type of argument used in against claim 1. Applicants disagree with this reasoning as per the response for claim 1.

With regard to claim 15, Applicants submit that element 603 of Childs is not a decoder and thus is not appropriate as being asserted as being analogous to the claimed decoder of claim 15.

Further with regard to claim 16 as amended, the analogy used by the Examiner is not a correct representation of the prior art. The Exclusive Or claimed is not analogous to that of Childs 605.

No amendment made was related to the statutory requirements of patentability unless expressly stated herein. No amendment made was for the purpose of narrowing the scope of any claim, unless Applicants have argued herein that such amendment was made to distinguish over a particular reference or combination of references.

Applicants believe the application is in condition for allowance which action is respectfully solicited. Please contact the below-signed if there are any issues regarding this communication or otherwise concerning the current application.

Respectfully submitted,

SEND CORRESPONDENCE TO:

Freescale Semiconductor, Inc.
Law Department

Customer Number: 23125

By: James L. Clingan, Jr.

James L. Clingan, Jr.
Attorney of Record
Reg. No.: 30,163
Telephone: (512) 996-6839
Fax No.: (512) 996-6854
Email: Jim.Clingan@Freescale.com